

Claims

1. A radio communication apparatus comprising:
 - a terminal interface unit for inputting data;
 - a radio communication control unit for inputting the data input by the terminal interface unit, for processing the data based on protocol, and outputting the data;
 - a confidentiality/integrity processing unit for inputting a control signal and data from the radio communication control unit, performing at least one of encryption of the data as confidentiality processing and generation of a message authentication code for detecting tampered data as integrity processing on the data input, and outputting the data processed to the radio communication control unit; and
 - a radio communication unit for inputting, modulating, and sending the data output from the radio communication control unit.
- 15 2. The radio communication apparatus of claim 1,
 - wherein the confidentiality/integrity processing unit inputs the control signal from the radio communication control unit and selectively inputs the data from the terminal interface unit based on the control signal input, and
 - 20 wherein the confidentiality/integrity processing unit performs confidentiality processing on the data input and outputs the data which has been performed confidentiality processing to the radio communication unit.
3. The radio communication apparatus of claim 2,
 - wherein the terminal interface unit outputs transparent data and
 - 25 non-transparent data, and

wherein the radio communication control unit inputs the non-transparent data from the terminal interface unit, makes the confidentiality/integrity processing unit process the non-transparent data based on protocol, and

5 wherein the radio communication control unit controls the transparent data to be transferred from the terminal interface unit to the confidentiality/integrity processing unit to perform the confidentiality processing.

4. The radio communication apparatus of claim 1, wherein the
10 confidentiality/integrity processing unit is connected to the radio communication control unit via parallel interface.

5. The radio communication apparatus of claim 1, wherein the confidentiality/integrity processing unit is connected to the terminal interface unit with serial interface and connected to the radio
15 communication unit with serial interface.

6. The radio communication apparatus of claim 1, wherein the confidentiality/integrity processing unit further includes:

 a confidentiality processing unit including an encrypting unit for encrypting the data input; and

20 an integrity processing unit having a message authentication code appending unit for appending a message authentication code to the data input.

7. The radio communication apparatus of claim 6, wherein the confidentiality/integrity processing unit includes multiple encrypting units.

25 8. The radio communication apparatus of claim 6, wherein the

20250732926500

confidence/integrity processing unit includes multiple message authentication code appending units.

9. The radio communication apparatus of claim 6, wherein the confidentiality processing unit and the integrity processing unit form one module which inputs the control signal and the data from the radio communication control unit, and the module performs at least one of the confidentiality processing and the integrity processing on the data input based on the control signal input.

10. A radio communication apparatus comprising:

10 a radio communication unit for receiving and demodulating data;
a radio communication control unit for inputting data demodulated by the radio communication unit, processing the data based on protocol, and outputting the data processed;
a confidentiality/integrity processing unit for inputting a control signal and the data from the radio communication control unit, based on the control signal input performing at least one of confidentiality processing of decrypting the data and integrity processing of detecting tampered data, and outputting the data processed to the radio communication control unit;
a terminal interface unit for inputting the data processed from the radio communication control unit and outputting the data.

20 11. The radio communication apparatus of claim 10,

wherein the confidentiality/integrity processing unit inputs the control signal from the radio communication control unit and selectively inputs the data from the radio communication unit based on the control signal input, and

CONFIDENTIAL

wherein the confidentiality/integrity processing unit performs the confidentiality processing on the data input and outputs the data processed to the terminal interface unit.

12. The radio communication apparatus of claim 11,

5 wherein the radio communication unit outputs transparent data and non-transparent data,

wherein the radio communication control unit inputs the non-transparent data from the radio communication unit and makes the confidentiality/integrity processing unit process the non-transparent data
10 based on protocol, and

wherein the radio communication control unit controls the transparent data to be transferred from the radio communication unit to the confidentiality/integrity processing unit to perform the confidentiality processing.

15 13. The radio communication apparatus of claim 10, wherein the confidentiality/integrity processing unit is connected to the radio communication control unit with a parallel interface.

14. The radio communication apparatus of claim 11, wherein the confidentiality/integrity processing unit is connected to the terminal interface unit with a serial interface, and connected to the radio communication unit with a serial interface.
20

15. The radio communication apparatus of claim 10, wherein the confidentiality/integrity processing unit includes:

a confidentiality processing unit having a decrypting unit for
25 decrypting the data input; and

20250000000000000000000000000000

an integrity processing unit having an integrity verification unit for verifying an integrity of the data input using a message authentication code appended to the data input.

16. The radio communication apparatus of claim 15, wherein the
5 confidentiality processing unit includes multiple decrypting units.

17. The radio communication apparatus of claim 15, wherein the integrity processing unit includes multiple integrity verification units.

18. The radio communication apparatus of claim 15, wherein the confidentiality processing unit and the integrity processing unit form one
10 module which inputs the control signal and the data from the radio communication control unit, and wherein the module, based on the control signal input, performs at least one of processes of the confidentiality processing unit and the integrity processing unit on the data input.

19. A radio communication apparatus for wireless data communication
15 comprising:

a terminal interface unit for data input/output;

a radio communication control unit for processing the data based on protocol;

a radio communication unit for wireless data communication; and

20 a confidentiality/integrity processing unit, provided among the terminal interface unit, the radio communication control unit, and the radio communication unit, which performs at least one of confidentiality processing for encrypting/decrypting data and integrity processing for detecting tampered data on the data input/output from/to the radio
25 communication control unit, encrypts the data from the terminal interface

P02900-02000-00000

unit to the radio communication unit, and decrypts the data from the radio communication unit to the terminal interface unit.

20. The radio communication apparatus of claim 19, wherein the confidentiality/integrity processing unit includes a confidentiality processing unit for performing a confidentiality processing on the data input, and an integrity processing unit for performing an integrity processing on the data input, separately.

21. The radio communication apparatus of claim 19, wherein the confidentiality processing unit separately includes an encrypting unit for encrypting the data from the terminal interface unit to the radio communication unit, and a decrypting unit for decrypting the data from the radio communication unit to the terminal interface unit.

22. The radio communication apparatus of claim 19, wherein the integrity processing unit separately includes a message authentication code appending unit for appending a message authentication code to the data input for performing an integrity processing, and an integrity verification unit for verifying an integrity of the data input using the message authentication code appended to the data input.

23. The radio communication apparatus of claim 19, wherein the communication apparatus is a portable mobile phone.

24. The radio communication apparatus of claim 6, wherein the confidentiality processing unit and the integrity processing unit employ same encryption algorithm.

25. The radio communication apparatus of claim 15, wherein the confidentiality processing unit and the integrity processing unit employ

20292665

same encryption algorithm.

26. The radio communication apparatus of claim 20, wherein the confidentiality processing unit and the integrity processing unit employ same encryption algorithm.

5 27. The radio communication apparatus of claim 1, wherein the communication apparatus is a cellular phone.

28. The radio communication apparatus of claim 10, wherein the radio communication apparatus is a cellular phone.

10 29. The radio communication apparatus of claim 19, wherein the communication apparatus is a cellular phone.

30. The radio communication apparatus of claim 1, wherein the radio communication apparatus is a radio station for sending/receiving data to/from a mobile station.

15 31. The radio communication apparatus of claim 10, wherein the radio communication apparatus is a radio station for sending/receiving data to/from a mobile station.

32. The radio communication apparatus of claim 19, wherein the radio communication apparatus is a radio station for sending/receiving data to/from a mobile station.

20 33. The radio communication apparatus of claim 30, wherein the radio station is either of a base transceiver station and a radio network controller.

34. The radio communication apparatus of claim 31, wherein the radio station is either of a base transceiver station and a radio network controller.

35. The radio communication apparatus of claim 32, wherein the radio 25 station is either of a base transceiver station and a radio network controller.

P00000000000000000000000000000000

36. A radio communication method comprising:

a terminal interface step for inputting data;

a radio communication control step for inputting the data input by the terminal interface step and for processing the data based on protocol and outputting the data;

5 a confidentiality/integrity processing step for inputting a control signal and data from the radio communication step, performing at least one of encryption of the data as confidentiality processing and generation of a message authentication code for detecting tampered data as integrity processing on the data input, and outputting the data processed to the radio communication control step; and

10 a radio communication step for inputting, modulating, and sending the data output from the radio communication control step.

37. A radio communication method comprising:

15 a radio communication step for receiving and demodulating data;

a radio communication control step for inputting data demodulated by the radio communication step, processing the data based on protocol, and outputting the data processed;

20 a confidentiality/integrity processing step for inputting a control signal and the data from the radio communication control step, based on the control signal input performing at least one of confidentiality processing of decrypting the data and integrity processing of detecting tampered data, and outputting the data processed to the radio communication control step; and

25 a terminal interface step for inputting the data processed from the radio communication control step and outputting the data.

38. A radio communication method for wireless data communication comprising:

- a terminal interface step for data input/output;
- a radio communication control step for data processing based on 5 protocol;
- a radio communication step for wireless data communication; and
- a confidentiality/integrity processing step, provided among the terminal interface step, the radio communication control step, and the radio communication step, and which performs at least one of confidentiality 10 processing for encrypting/decrypting data and integrity processing for detecting tampered data on the data input/output from/to the radio communication control step, encrypts the data transferred from the terminal interface step to the radio communication step, and decrypts the data transferred from the radio communication step to the terminal interface 15 step.

FOV2000-A00000000000